



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/761,771	01/18/2001	Virgil Dorin Gligor	068398/0102	5946

7590 12/23/2004  
William T. Ellis  
FOLEY & LARDNER  
Washington Harbour  
3000 K Street, N.W., Suite 500  
Washington, DC 20007-5109

EXAMINER

TRAN, TONGOC

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 12/23/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

Application No.

09/761,771

Applicant(s)

GLIGOR ET AL.

Examiner

Tongoc Tran

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☐ Responsive to communication(s) filed on 20 August 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-82 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-82 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date 7/17/2001, 11/13/2.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_.

### **DETAILED ACTION**

1. This Office Action is in response to Applicant's application serial no. 09/761,771 filed on 1/18/2001 and preliminary amendment filed on 8/20/2001. Claims 65-82 are added. Claims 1-82 are pending.

### ***Information Disclosure Statement***

2. The information disclosure statement (IDS) submitted on 7/17/2001 and 11/13/2001 have been considered by the examiner.

### ***Claim Objections***

3. Claim 4 is objected to because of the following informalities:

The term "an" appears to be a typographical error. Appropriate correction is required.

### ***Specification***

4. The disclosure is objected to because it contains an embedded hyperlink and/or other form of browser-executable code. Applicant is required to delete the embedded hyperlink and/or other form of browser-executable code. See MPEP § 608.01.

### ***Claim Rejections - 35 USC § 102***

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

Art Unit: 2134

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1, 2, 6, 8-9, 21-25, 28-29, 30-31, 34, 47-48, 50-53, 55-56 and 65-81 are rejected under 35 U.S.C. 102(b) as being anticipated by Jueneman ("Message Authentication", Proceedings of the 1983 IEEE Symposium on Security and Privacy, hereinafter Jueneman).

In respect to claims 1, 28 and 65, Jueneman discloses an encryption and the inverse of the encryption method for providing both data confidentiality and integrity for a message, comprising the steps of:

receiving an input plaintext string comprising a message and padding it as necessary such that its length is a multiple of  $\ell$  bits; partitioning the input plaintext string a length that is a multiple of  $\ell$  bits into a plurality of equal-size blocks of  $\ell$  bits in length (see page 37, col. 1, last paragraph-page 38, 2<sup>nd</sup> paragraph).

creating an MDC block of  $\ell$  bits in length that includes the result of applying a non-cryptographic Manipulation Detection Code (MDC) function to the plurality of the equal-size blocks; making one and only one processing pass with a single cryptographic primitive over each of said equal-size blocks and the MDC block to create a plurality of hidden ciphertext blocks each of  $\ell$  bits in length and performing a randomization function over said plurality of hidden ciphertext blocks to create a plurality of output ciphertext blocks each of  $\ell$  bits in length (see Abstract, page 40, col. 1, 3<sup>rd</sup> paragraph-page 41, 3<sup>rd</sup> paragraph).

Verifying integrity of the plaintext blocks using a non-cryptographic Manipulation Detection Code (MDC) function; outputting the plurality of plaintext blocks as an

Art Unit: 2134

accurate plaintext string if the integrity verification passes; and outputting a failure indicator if the integrity verification fails (see page 40, col. 1, 3<sup>rd</sup> paragraph-page 41, col. 1, 4<sup>th</sup>).

In respect to claims 2, 29 and 66, Jueneman discloses the method as defined in claims 1 and 28 comprising the steps of encryption and reverse encryption:

wherein said making one and only one processing pass step comprises processing each of said equal-size blocks and the MDC block by an encryption scheme that is confidentiality-secure against chosen-plaintext attacks, wherein each of said equal-size blocks and the MDC block is processed by a block cipher using a first secret key to obtain said plurality of hidden ciphertext blocks; and wherein said performing a randomization function step comprises combining each of said hidden ciphertext blocks with a corresponding element of a sequence of unpredictable elements to create a set of output blocks of the ciphertext, wherein a hidden ciphertext block identified by an index  $i$  is combined with the element of the sequence identified by index  $i$  by an operation that has an inverse (see page 37, col. 1, last paragraph-page 41, 4<sup>th</sup> paragraph and page 47, col. 1, 3<sup>rd</sup> paragraph-col. 2, 2<sup>nd</sup> paragraph).

In respect to claim 6, Jueneman discloses the method as defined in claim 2, further comprising the step of appending the created MDC block after a last block of the set of equal-sized blocks comprising the padded plaintext string (page 37, col. 2, last paragraph).

In respect to claim 8, Jueneman discloses the method as defined in claim 2, wherein the hidden ciphertext blocks from the processing step comprise  $n+1$  hidden

Art Unit: 2134

ciphertext blocks each of  $\ell$ -bit length, where  $n$  is the total number of blocks in said set of equal-sized blocks of the padded input plaintext string (see Jueneman, page 40, col. 1, 3<sup>rd</sup> paragraph-page 41, col. 1, 4<sup>th</sup> paragraph).

In respect to claim 9, Jueneman discloses a method as defined in claim 2, further comprising the step of generating each of a plurality of the unpredictable elements of said sequence of unpredictable elements by combining a different element identifier for each of the unpredictable elements and a secret random number (see page 37, col. 1, last paragraph-page 41, 4<sup>th</sup> paragraph and page 47, col. 1, 3<sup>rd</sup> paragraph-col. 2, 2<sup>nd</sup> paragraph).

In respect to claim 21, Jueneman discloses the method as defined in claim 1, wherein said non-cryptographic MDC function is a bit-wise exclusive-or function (see Jueneman, page 40, col. 1, 3<sup>rd</sup> paragraph-page 41, col. 1, 4<sup>th</sup> paragraph).

In respect to claim 22, Jueneman discloses the method as defined in claim 2, wherein said encryption scheme is the CBC scheme of encryption (Jueneman, page 40, col. 1, 3<sup>rd</sup> paragraph-page 41, col. 1, 4<sup>th</sup> paragraph).

In respect to claim 23, Jueneman discloses the method as defined in claim 2, wherein said operation that has an inverse is the addition modulo  $2^{\text{sup. } \ell}$  (see Jueneman, page 45, col. 1, 3<sup>rd</sup> paragraph-page 46, col. 1, 1<sup>st</sup> paragraph).

In respect to claim 24, Jueneman discloses the method as defined in claim 2, wherein said operation that has an inverse is a bit-wise exclusive-or operation (see Jueneman, col. 40, col. 1, 3<sup>rd</sup> paragraph-page 41, col. 1, 4<sup>th</sup> paragraph).

In respect to claim 25, Jueneman discloses the method as defined in claim 2, wherein said operation that has an inverse is the subtraction modulo 2.sup.  $\ell$  operation (see Jueneman, page 45, col. 1, 3<sup>rd</sup> paragraph-page 46, col. 1, 1<sup>st</sup> paragraph).

In respect to claim 30, Jueneman discloses the method of claim 28, further comprising: selecting the ciphertext block of a secret random number from said string presented for decryption; and deciphering the selected ciphertext block to obtain the secret random number (see page 40, col. 1, 3<sup>rd</sup> paragraph-page 41, col. 1, 4<sup>th</sup> paragraph).

In respect to claim 31, Jueneman discloses the method as defined in claim 30, wherein said deciphering step comprises performing the deciphering with the inverse of the said block cipher using the secret first key (see page 40, col. 1, 3<sup>rd</sup> paragraph-page 41, col. 1, 4<sup>th</sup> paragraph).

In respect to claim 34, Jueneman discloses the method as defined in claim 28, wherein the string presented for decryption is obtained by applying the encryption method that provides both data confidentiality and integrity to an input plaintext string, further comprising: outputting said input plaintext string (see page 40, col. 1, 3<sup>rd</sup> paragraph-page 41, col. 1, 4<sup>th</sup> paragraph).

In respect to claims 47-48, the claim limitations are program product claims that are similar to method claims 1-2. Therefore, claims 47-48 are rejected based on the similar rationale.

In respect to claims 50-51, the claim limitations are program product claims that are similar to method claims 28-29. Therefore, claims 50-51 are rejected based on the similar rationale.

In respect to claims 52-53, the claim limitations are system claims that are similar to method claims 1-2. Therefore, claims 52-53 are rejected based on the similar rationale.

In respect to claims 55-56, the claim limitations are system claims that are similar to method claims 28-29. Therefore, claims 55-56 are rejected based on the similar rationale.

In respect to claim 67, Jueneman discloses the method as defined in claim 65, wherein said generating a plurality of equal-sized blocks of  $\ell$  bits in length from the input plaintext string further comprises the steps of:

padding the input plaintext string as necessary such that its length is a multiple of  $\ell$  bits; and partitioning the padded input plaintext string into a plurality of equal-size blocks of  $\ell$  bits in length (see page 37, col. 2, 4<sup>th</sup> paragraph).

In respect to claim 68, Jueneman discloses the method as defined in claim 67, wherein said padding of the input plaintext string is a standard padding method (see page 37, col. 2, 4<sup>th</sup> paragraph).

In respect to claims 69-70, 76 and 82, Jueneman discloses the method, program product and system as defined in claim 66, 2, 48 and 53, wherein the result of the combination of any two different unpredictable elements of the sequence of unpredictable elements by the inverse operation of the operation to create a set of



Art Unit: 2134

output blocks of the ciphertext is unpredictable; and wherein said unpredictable elements selected as said two unpredictable elements are any two different elements of the same sequence of unpredictable elements used for the encryption of said plaintext string; and wherein said unpredictable elements selected as said two unpredictable elements are any two different elements of a plurality of sequences of unpredictable elements used for encryption of a plurality of plaintext strings with the same secret key K (see page 37, col. 1, last paragraph-page 41, 4<sup>th</sup> paragraph and page 47, col. 1, 3<sup>rd</sup> paragraph-col. 2, 2<sup>nd</sup> paragraph).

In respect to claims 71-75, the claim limitations are program product claims that are similar to method claims 65-69. Therefore, claims 71-75 and 77-81 are rejected based on the similar rationale.

In respect to claims 77-81, the claim limitations are system claims that are similar to method claims 65. Therefore claims 77-81 are rejected based on the similar rationale.

### ***Claim Rejections - 35 USC § 103***

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 3-5, 7, 10-20, 26-27, 32-33, 49 and 54 are rejected under 35 U.S.C.

103(a) as being unpatentable over Jueneman ("Message Authentication", Proceedings

of the 1983 IEEE Symposium on Security and Privacy, hereinafter Jueneman) in view of Jakubowski et al. (U.S. Patent No. 6,226,742).

In respect to claims 3 and 5, Jueneman discloses the method as defined in claim 2, wherein said creating an MDC block step comprises:

applying the non-cryptographic MDC function to the partitioned plaintext blocks; and combining the result with a secret  $\ell$ -bit random vector to obtain said MDC block (see page 40, 3<sup>rd</sup> paragraph-page 41, col. 1, 4<sup>th</sup> paragraph).

Jueneman does not explicitly disclose but Jakubowski discloses comprising the step of generating said secret random vector from a secret random number generated on a per-message basis (see Jakubowski, col. 9, lines 4-58). It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement Jakubowski's generating secret random vector on a per-message basis for better protection of message in known plaintext attack.

In respect to claim 4, Jueneman and Jakubowski disclose the method as defined in claim 3, wherein said combining step comprises performing the combination using a bit-wise exclusive-or function (see page 40, 3<sup>rd</sup> paragraph-page 41, col. 1, 4<sup>th</sup> paragraph).

In respect to claim 7, Jueneman and Jakubowski disclose the method as defined in claim 3, wherein said encryption scheme is cipher block chaining (CBC) further comprising the step of representing an initialization vector for the CBC as the secret random vector (see page 40, 3<sup>rd</sup> paragraph-page 41, 4<sup>th</sup> paragraph).

In respect to claim 10, Jueneman and Jakubowski disclose the method as defined in claim 5, further comprising the step of generating each of a plurality of the unpredictable elements of said sequence of unpredictable elements by combining a different element identifier for each of the unpredictable elements and said secret random number (see Jakubowski, col. 9, lines 4-58).

In respect to claim 11, Jueneman and Jakubowski disclose the method as defined in claim 5, further comprising the steps of: enciphering the secret random number using the block cipher using the secret first key; and including this enciphered secret random number as one of said output ciphertext blocks (see Jakubowski, col. 9, lines 4-58).

In respect to claim 12, Jueneman and Jakubowski disclose the method of claim 3, wherein said secret random vector is generated by enciphering a secret random number of  $\ell$  bits in length, said enciphering using said block cipher using a secret second key (see Jueneman, page 37, 4<sup>th</sup> paragraph-page 38, 2<sup>nd</sup> paragraph).

In respect to claim 13, Jueneman and Jakubowski disclose the method as defined in claim 5, wherein said secret random vector is generated by enciphering a variant of said secret random number of bits in length, said enciphering using said block cipher using said secret first key (see Jakubowski, col. 9, lines 4-58).

In respect to claim 14, Jueneman and Jakubowski disclose the method as defined in claim 13, wherein said variant of said secret random number is obtained by adding a constant to said secret random number (see Jakubowski, col. 9, lines 4-58 and col. 11, lines 1-40).

In respect to claim 15, Jueneman and Jakubowski disclose the method of claim 5, wherein the secret random number is provided by a random number generator (see Jakubowski, col. 9, lines 4-33).

In respect to claim 16, Jueneman and Jakubowski disclose the method as defined in claim 5, further comprising: generating said secret random number by enciphering a count of a counter initialized to a constant, said enciphering being performed with the block cipher using the secret first key; and incrementing said counter by one on every message encryption (see Jakubowski, col. 16, lines 37-58).

In respect to claim 17, Jueneman and Jakubowski disclose the method as defined in claim 16, wherein said counter is initialized to a constant whose value is the  $\ell$ -bit representation of negative one (see Jakubowski, col. 14, line 61-col. 15, line 14).

In respect to claim 18, Jueneman and Jakubowski disclose the method as defined in claim 16, comprising: initializing said counter to a secret value of  $\ell$  bits in length (see Jakubowski, col. 14, line 61-col. 15, line 14).

In respect to claim 19, Jueneman and Jakubowski disclose the method as defined in claim 16, further comprising: outputting said counter value as an output block of the encryption scheme (see Jakubowski, col. 14, lines 4-27).

In respect to claim 20, Jueneman and Jakubowski disclose the method as defined in claim 5, further comprising: sharing the secret random number between a sender and a receiver (see Jakubowski, col. 9, lines 34-58).

In respect to claim 26, Jueneman and Jakubowski disclose the method as defined in claim 3, further comprising: generating said secret random vector from a

secret random number of  $\ell$ -bit length; and generating each element in said sequence of unpredictable elements by modular  $2^{\text{sup. } \ell}$  multiplication of a different unique element identifier (i) for each element in the sequence of unpredictable elements and said secret random number (see Jueneman, page 47, 4<sup>th</sup> paragraph-page 49, col. 1, 3<sup>rd</sup> paragraph).

In respect to claim 27, Jueneman and Jakubowski disclose the method as defined in claim 3, further comprising: generating said secret random vector from a secret random number of  $\ell$ -bit length; and generating each element in said sequence of unpredictable elements from the previous element by modular  $2^{\text{sup. } \ell}$  addition of said secret random number to the previous element, with a first element of said sequence being said secret random number itself (see Jueneman, page 47, 4<sup>th</sup> paragraph-page 49, col. 1, 3<sup>rd</sup> paragraph).

In respect to claims 32-33, the claim limitation is similar to claim 16. Therefore, claim 29 is rejected based on the similar rationale.

In respect to claim 49, the claim limitation is a program product claim that is similar to method claim 3. Therefore, claim 49 is rejected based on the similar rationale.

In respect to claim 54, the claim limitation is a system claim that is similar to method claim 3. Therefore, claim 54 is rejected based on the similar rationale.

7. Claims 35-36, 41-44 and 57-64 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jueneman ("Message Authentication", Proceedings of the 1983 IEEE Symposium on Security and Privacy, hereinafter Jueneman) in view of Enichen et al. (U.S. Patent No. 6,333,983).

In respect to claims 35 and 41, Jueneman discloses method for encryption and inverse encryption processing of a message comprising the steps of: partitioning said input plaintext string into a plurality of input plaintext segments;

presenting each different one of said plurality of input plaintext segments to a different one of a plurality of encryption processors, each of said different processors using a different  $\ell$ -bit secret random number per segment to obtain a ciphertext segment using an encryption method providing both data confidentiality and integrity with a single processing pass over the input plaintext segment and a single cryptographic primitive, and using a non-cryptographic Manipulation Detection Code function, wherein said single cryptographic primitive is a  $\ell$ -bit block cipher using a secret first key; assembling the plurality of ciphertext segments into a ciphertext string; and outputting the ciphertext string (see page 37, col. 1, last paragraph-page 38, 2<sup>nd</sup> paragraph).

Assembling the plurality of plaintext segments into plaintext string; and verifying the integrity of the plaintext segment and their sequence and outputting the plaintext string if the integrity verification passes (see page 40, col. 1, 3<sup>rd</sup> paragraph-page 41, col. 1, 4<sup>th</sup>).

Jueneman does not disclose but Enichen discloses using parallel processing to implement the encryption and decryption processes (see Enichen, col. 2, lines 40-60). It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement parallel processing in cryptographic application taught by Enichen with Jueneman's teaching of message authentication with manipulation

detection code to minimize time consuming encryption and decryption processes for speedier processing.

In respect to claim 36, Jueneman and Enichen discloses the method as defined in claim 35, wherein said assembling step comprises including in the ciphertext string the number of ciphertext segments, a ciphertext segment index, a length of each ciphertext segment and a sequence of ciphertext segments (see page 40, col. 1, 3<sup>rd</sup> paragraph-page 41, col. 1, 4<sup>th</sup>).

In respect to claim 42, Jueneman and Enichen disclose the method as defined in claim 41, further comprising outputting a failure indicator if the integrity verification fails for at least one segment (see Jueneman page 40, col. 1, 3<sup>rd</sup> paragraph-page 41, col. 1, 4<sup>th</sup>).

In respect to claim 43, Jueneman and Enichen disclose the method of claim 41, further comprising: selecting a ciphertext block of the secret random number from said string presented for decryption; deciphering the selected ciphertext block to obtain the secret random number verification fails for at least one segment (see Jueneman page 40, col. 1, 3<sup>rd</sup> paragraph-page 41, col. 1, 4<sup>th</sup>).

In respect to claim 44, Jueneman and Enichen disclose the method as defined in claim 43, performing said deciphering step with the inverse of a block cipher using a secret first key, said block cipher and said secret first key being the same as to those used at the message encryption method using the plurality of processors (see Jueneman, page 38, col. 1, 3<sup>rd</sup> paragraph-page 39, col. 2, 2<sup>nd</sup> paragraph and 40, col. 1, 3<sup>rd</sup> paragraph-page 41, col. 1, 4<sup>th</sup>).

In respect to claims 57-58, the claim limitations are program product claims that are similar to method claims 35-36. Therefore, claims 57-58 are rejected based on the similar rationale.

In respect to claims 59-60, the claim limitations are program product claims that are similar to method claims 41-42. Therefore, claims 59-61 are rejected based on the similar rationale.

In respect to claims 61-62, the claim limitations are system claims that are similar to method claims 35-36. Therefore, claims 61-62 are rejected based on the similar rationale.

In respect to claims 63-64, the claim limitations are system claims that are similar to method claims 41-42. Therefore, claims 63-64 are rejected based on the similar rationale.

8. Claims 37-40 and 45-46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jueneman ("Message Authentication", Proceedings of the 1983 IEEE Symposium on Security and Privacy, hereinafter Jueneman) in view of Enichen et al. (U.S. Patent No. 6,333,983) and further in view of Jakubowski et al. (U.S. Patent No. 6,226,742).

In respect to claim 37, Jueneman and Enichen disclose the method of claim 35. Jueneman and Enichen do not explicitly disclose but Jakubowski discloses generating said different  $\ell$ -bit secret random number per segment from a secret random number of  $\ell$ -bits in length (see Jakubowski, col. 9, lines 4-58). It would have been obvious to one



of ordinary skill in the art at the time the invention was made to implement Jakubowski's generating secret random vector on a per-message basis for better protection of message in known plaintext attack.

In respect to claim 38, Jueneman, Enichen and Jakubowski disclose the method of claim 37, further comprising: generating said different secret random number per segment from the secret random number of  $\ell$  bits by adding modulo 2.sup.  $\ell$  a plaintext segment sequence index for that segment to the secret random number (see Jueneman, page 45, col. 1, 3<sup>rd</sup> paragraph-page 46, col. 1, 1<sup>st</sup> paragraph).

In respect to claim 39, Jueneman, Enichen and Jakubowski disclose the method of claim 37, further comprising: generating said secret random number of  $\ell$  bits in length by a random number generator; enciphering said secret random number with said block cipher using a first key; and including the enciphered secret random number as an output block of said output ciphertext string (see Jakubowski, col. 9, lines 4-59).

In respect to claim 40, Jueneman, Enichen and Jakubowski disclose the method of claim 37, further comprising: generating said secret random number of  $\ell$  bits in length by enciphering a counter initialized to a constant, said enciphering being done with said block cipher using said first key; and outputting said counter value as an output block of said output ciphertext string; and incrementing after every different message encryption said counter by a number equal to a number of plaintext segments in the message (see Jakubowski, col. 14, line 5-col. 15, line 14).

In respect to claims 45-46, the claim limitations are similar to claim 40. Therefore, claims 45-46 are rejected based on the similar rationale.

Art Unit: 2134

**Conclusion**

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tongoc Tran whose telephone number is (571) 272-3843. The examiner can normally be reached on 8:30-5:00 M-F.

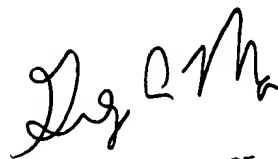
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached at (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Examiner: Tongoc Tran  
Art Unit: 2134

TT

  
December 9, 2004

  
GREGORY MORSE  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2134